Közlemenyek 29/1983 75-91

THE ALGEBRAIC STRUCTURE OF PRIMITIVE RECURSIVE FUNCTIONS

István Szalkai

student of Eötvös Loránd University,

Budapest

ABSTRACT

In this article I looked at the set of primitive recursive functions as an algebraic structure with two operations: composition o and iteration □, see below. I prove that there is no endomorphism on this structure besides ID and $\underline{O}$ (see Theorem I). After this I prove that certain sets of functions from N to N (for example the set of primitive recursive functions) cannot be generated with one function with the help of operations o and □ (see Theorem II and III). In my paper I also write some problems concerning this topic.

INTRODUCTION

Denote by N the set of non-negative integers. We say that the function f is generated from the functions g and h by primitive recursion if there is a k such that

$$f : \mathrm{N}^{k+1} \to \mathrm{N},\ g : \mathrm{N}^{k+2} \to \mathrm{N},\ h : \mathrm{N}^{k} \to \mathrm{N}$$

and for every $\underline{m} \in \mathrm{N}^{k} : f(0,\underline{m})=h(\underline{m})$ and $f(n+1,\underline{m})=g(n,\underline{m},f(n,\underline{m}))$. Let us define three special functions as follows:

$$
\begin{array}{llll}
\underset{\sim}{O} : \mathrm{N} \to \{0\} & i.e. & \forall n \in \mathrm{N} & \underset{\sim}{O}(n)=0 \\
S : \mathrm{N} \to \mathrm{N} & : & \forall n \in \mathrm{N} & S(n)=n+1 \\
\underline{\bullet} : \mathrm{N} \to \mathrm{N} & : & \forall n \in \mathrm{N} & \underline{\bullet}(n)= \begin{cases} n-1 & if \quad n \geq 1 \\ 0 & otherwise \end{cases}
\end{array}
$$

These are called basic functions.

In general denote by $\underset{\sim}{c}$ the constant function from N to N having the value c, $c \in$ N.

A function f from N^k to N, $k \geq 1$, is called primitive recursive if it can be generated from the basic functions with the help of primitive recursion, composition and projections from N^k to N in finite steps. Since there is a calculable (i.e. primitive recursive) bijection between N^k and N we can restrict ourselves to functions from N to N. Denote by PR the set of the primitive recursive functions from N to N. For the usual definition of primitive recursive functions see [2], [4] or [5].

For an arbitrary function f from N to N denote by $f^{\square}$ the "iterand-function" of f from 0, i.e. let $f^{\square}(0)=0$ and for every n, $f^{\square}(n+1)=f(f\ (n))$. Furthermore we shall denote by quadres (n) the quadratic residuum of n, i.e. the distance between n and the greatest square number no greater than n. For example quadres $(16)=0$, quadres $(53)=4$, etc. Denote by o the operation of composition and by + the operation of addition of two functions. R.M. Robinson [1] proved that every primitive recursive function from N to N can be generated from the basic function S and the quadres with the help of the operations o, + and
The starting point of my investigations was this fact. Denote by $<PR,o,\square>$ the set PR as an algebraic structure with operations o and $\square$. The main purpose of this paper is to investigate the algebraic properties of $<PR,o,\square>$.

It is easy to see that $<PR,o>$ is a semigroup with a unit element id (since $id=S^{\square} \in PR$), where the only left-hand-singular elements are the constant ones and there is no right-hand-singular element. Obviously $\square$ is a unary operation from PR to PR and $Ker\,\square \supset Im$. It easy to see that $Ker\,\square = \{f:f(0)=0\}$ and *quadres* $\in Ker\square\setminus Im\square$.

For every f $f^{\square\square}=\underset{\sim}{0}$, so the only fixpoint of $\square$ is $\underset{\sim}{0}$. (To prove this we have to use algebraic considerations only: we have to observe that if $f^{\square}=f$ then $f^{\square\square}=f$ and $\underset{\sim}{0}=f^{\square\square}=f^{\square}=f$.)

If $= <A,g_1,\dots,g_m>$ is an arbitrary algebraic structure, then every homomorphism from A to A is called endomorphism. Denote by $End(\quad)$ the set of these endomorphisms. The identity operation ID on A (i.e. $ID(a)=a$ for every $a\in A$) is trivially an element of $End(\quad)$. If   contains a null element 0 for every operations of   then the null-operation $\underline{0}$ (i.e. $\underline{0}(a)=0$ for every element of A) is also an endomorphism on . It is obvious that $\underset{\sim}{0}$ is the null element of PR, i.e. $\underset{\sim}{0}\circ\underset{\sim}{0}=\underset{\sim}{0}$ and $\underset{\sim}{0}^{\square}=\underset{\sim}{0}$. So we got that ID and $\underline{0}$ are elements of $End<PR,o,\ >$. In the next section I prove that $End<PR,o,\square>=\{\underline{0},ID\}$ (see Theorem I). After this I examine a more general question: what are the similar structures such that for them this theorem holds (see Theorem I.A and I.B). As I know well, these questions have not been investigated yet. Only the automorphisms of degrees were studied in [5] and [6]. In this paper I investigate the structure of null degree itself.

Above we have seen two equivalent definitions of primitive recursive functions (the usual one and the definition of R.M. Robinson.) There are still more equivalent definitions of them (see [3], [4]) and there are a lot of open problems concerning how to generate PR in a more simple way. I prove a theorem concerning this (see Theorem II) which seems to be an interesting one.

Namely the theorem says the following:

In what follows denote by $<a>$ the set of functions f from N to N which can be built from the function a with the help of operations o and $\square$ in finite steps. Let a be an arbitrary function from N to N. Then the Theorem says that

either there is no bijection in $<a>$

or $\forall f\in<a>$ f is either injective or $R(f)$ is finite.

($R(f)$ denotes the range of f, i.e. $R(f)=\{f(i):i\in \mathrm{N}\}$). Denote by PR^+ the monotone increasing elements of PR. The corollary of the above Theorem says that there is no $a\in PR$ such that $\langle a\rangle=PR$ or $\langle a\rangle=PR^+$ (see Theorem III). It is not known whether the operation + can be eliminated from the definition of primitive recursive functions or not. To be more exact the problem is the following:

PROBLEM 1.: Are there $u,v\in PR$ such that PR can be generated from the functions u and v with the help of the operations o and ?

To solve this problem I suggest to choose another σ_2^1 (see in [2], §.7.16.)

If such u and v exist then Theorem III implies that the result of R.M.Robinson is sharp. A similar result was proved in [3], Theorem 6. Let f^{-1} (inversion) denote the following operation: for every surjective f let f^{-1} be a function such that $f^{-1}(x)=min\{y:f(y)=x\}$. J.Robinson [3] proved that R cannot be generated from only one function with the help of operations o and f^{-1} (R denotes the set of general recursive functions). In her proof she eliminated the operation + with the help of a *, a "mirror-operation".

My Theorem I shows that her method is not applicable in our case because * is an endomorphism on R.

The results of this paper seem to be the first ones concerning the properties of $\langle PR,o,\square\rangle$. I think it is interesting and useful to investigate similar problems, for example

to study other properties of the operators o and $\square$

to investigate other operations on PR

(for example $(\Sigma f)(n)=f(0)+f(1)+\ldots+f(n)$ or f^{-1})

to raise other usual and unusual algebraic questions in the algebraic structure $\langle PR,o,\square\rangle$, etc.

I thank Emil W. Kiss and B. Uhrin for their useful remarks.

ENDOMORPHISMS

The main purpose of present section is to prove Theorem I. To do this we need some abbreviations and two lemmas, but first I explain some remarks on the endomorphisms on PR.

Let $c \in N$, $c \neq 0$ and let L be the following endomoprhism: for $\forall f \in PR$ let $L(f)=\underset{\sim}{c}$ i.e. $L:PR \to \{\underset{\sim}{c}\}$. Since $\underset{\sim}{c}$ is a left-hand-singular element of PR, so it is easy to see that $L \in End\langle PR,o\rangle$. Since $\underset{\sim}{c}^{\square}(0)=0$ so $\underset{\sim}{c}^{\square} \neq \underset{\sim}{c}$ so $L \notin End\langle PR,\square\rangle$ i.e. we have got that $L \in End\langle PR,o\rangle \setminus End\langle PR,\square\rangle$. Conversely let $\hat{s}g=(So\underset{\sim}{0})^{\square}$ be the usual signum function: $sg(0)=0$ and $sg(n)=1$ for $n \neq 0$.

Let $L(f)=sgofosg$ for every $f \in PR$. Then it is easy to see that $L \in End\langle PR,\square\rangle$. (We have to examine where f is equal to 0 and where it is not.) Furthermore by Lemma 1 we can say that $L \notin End\langle PR,o\rangle$ so $L \in End\langle PR,\square\rangle \setminus End\langle PR,o\rangle$. If we want an easier example for $L \in End\langle PR,\square\rangle \setminus End\langle PR,o\rangle$ then let $L(f)=f^{\square}$ for every $f \in PR$.

The following lemma is useful both to the above elementary investigations and to prove the main theorem.

LEMMA 1. Let $u,v \in PR$ be arbitrary functions such that $v\ u \neq id$ and u is not a constant function. Let $L(f)=u\ f\ v$ for every $f \in PR$. Then $L \notin End\langle PR,o\rangle$.

PROOF: Let $x_1,x_2,Z \in$ N be such that $(vou)(Z)=y \neq Z$ and $u(x_1) \neq u(x_2)$ Furthermore let $f,g \in PR$ be szch that

$$g(v(0))=Z \quad and \quad f(Z)=x_1, \quad f(y)=x_2.$$

Such f and g obviously exist. For example let $g(n)=0$ for $n \neq v(0)$ and $f(n)=0$ for $n \neq Z$ and $n \neq y$. From the usual definition of primitive recursive functions it is easy to see that if $f(n) \neq 0$ only for finite n then f is primitive recursive (see for example [2].)

Then $L(f\circ g)(0)=(u\circ f\circ g\circ v)(0)=u(x_1)\neq u(x_2)=(u\circ f\circ v\circ u\circ g\circ v)(0)$ $=(L(f)\circ L(g))(0)$

so $L(f\circ g)\neq L(f)\circ L(g)$ i.e. $L\notin End<PR,o>$. ■

Concerning this lemma the following problem arises:
PROBLEM 2: Are there functions u and v such that for every $f\in PR$:

$$f^{\square}=u\circ f\circ v \quad ?$$

The corollary of the next lemma will be useful for the proof of Theorem I.

LEMMA 2. Let $f\in PR$ and $f(0)=0$ Assume that f^{-1} exists (from this point f^{-1} will denote the usual invers function of f for the operations o, i.e. $f^{-1}\circ f=f\circ f^{-1}=id$.)
Furthermore let $f^{-1}\in PR$.
Then $\exists!$ $g\in PR$ such that $f=g^{\square}$.

PROOF: Let $g=f\circ S\circ f^{-1}$ then $g\in PR$ and $g^{\square}(n)=(f\circ S\circ f^{-1})\underbrace{\circ(f\circ S\circ f^{-1})\circ}_{n\ times}$

$\dots(f\circ S\circ f^{-1})(0)$ i.e. a suitable g exists.

If $f=g^{\square}$ then $f(n+1)=g^{\square}(n+1)=g(g^{\square}(n))=g(f(n))$ i.e. $f\circ S=g\circ f$ i.e. $f\circ S\circ f^{-1}=g$ i.e. there is only one correct g. ■

COROLLARY: $id=f^{\square}$ <=> $f=S$.

THEOREM I. If $L\in End<PR,o,\square>$ then $L=\underline{0}$ or $L=ID$.

PROOF: There are two cases:

a.) $L(id)=id$ and b.) $L(id)\neq id$

CASE a.) $L(id)=id$

Then $id=L(id)=L(S^{\Box})=(L(S))^{\Box}$ and from this we get that $L(S)=S$ using the corollary of Lemma 2. For every $c\in\mathrm{N}$ and function f from N to N let $f^{c}=\underbrace{f\circ f\circ\ldots\circ f}_{c\ times}$ for $c\neq 0$ and $f^{0}=id$.

For an arbitrary constant function $\underset{\sim}{c}$ $\underset{\sim}{c}=S^{c}\circ\underset{\sim}{0}$ and $L(\underset{\sim}{c})=L(S^{c}\circ\underset{\sim}{0})=L(S^{c}\circ id^{\Box})=L(S)^{c}\circ L(id)^{\Box}=S^{c}\circ id^{\Box}=S^{c}\circ\underset{\sim}{0}=\underset{\sim}{c}$.

Furthermore, for every $f\in PR$ and $c\in\mathrm{N}$ $\underset{\sim}{f(c)}=L(\underset{\sim}{f(c)})=L(f\circ\underset{\sim}{c})=L(f)\circ\underset{\sim}{c}==L(\underset{\sim}{f)(c})$

i.e. $f(c)=L(f)(c)$ which implies $f=L(f)$

i.e. $L=ID$.

CASE b.) $L(id)\neq id$

To spare place, for every $f\in PR$ denote $f'=L(f)$ and let $N'=\bigcup\{\mathrm{R}(f') : f\in PR\}$ i.e. all elements of N contained in $\mathrm{R}(f')$ for any $f\in PR$. At first I examine whether N' equalsto N or not. For every $f\in PR$ $id\circ f=f$ so $id'\circ f'=f'$ i.e. $\forall c\in\mathrm{N}$ $id'(f'(c))=f'(c)$. In other words $id'(d)=d$ if $d\in N'$ since $f'(c)\in N'$ or $\forall d\in N'$ $id'(d)=d$. Denote this fact by $id'\big|_{N'}=id\big|_{N'}$. Obviously by the definition of N',$\mathrm{R}(id')\subseteq N'$. Conversely $\forall d\in N'$ $id'(d)=d$ so $\mathrm{R}(id')\supseteq N'$ i.e. $\mathrm{R}(id')=N'$.

From this $N'\neq\mathrm{N}$ follows because $id'\big|_{N'}=id\big|_{N'}$ and $id'\neq id$.

Obviously $\underset{\sim}{0}'=(id^{\Box\Box})'=id'^{\Box\Box}=\underset{\sim}{0}$.

At this point we prove the following proposition: if $f'\big|_{N'}=g'\big|_{N'}$ (i.e. $\forall d\in N'$ $f'(d)=g'(d)$) then $f'=g'$.

Since for every $y\in\mathrm{N}$ $(f')(y)=(f'\ id')(y)=f'(id'(y))=g'(id'(y))=g'\ id')(y)=(g')(y)$ so $f'=g'$.

For every $a\in\mathrm{N}$ we know that

$$\underset{\sim}{a}'=(S^{a}\circ\underset{\sim}{0})'=S'^{a}\circ\underset{\sim}{0}=\underset{\sim}{S'^{\Box}}(a)=S'^{\Box}\circ\underset{\sim}{a}=S^{\Box'}\circ\underset{\sim}{a}=id'\circ\underset{\sim}{a}$$

i.e. (*) $\forall a\in N$ $id'\circ\underset{\sim}{a}'=id'\circ\underset{\sim}{a}$.

Especially if $a\in N'$ then $\underset{\sim}{a}'=\underset{\sim}{a}$.

Then $id'' \underset{\sim}{a} = id''\circ \underset{\sim}{a}' = (id'\circ \underset{\sim}{a})' = (\underset{\sim}{a})' = \underset{\sim}{a}' = \underset{\sim}{a}$

so $id''\big|_{N'} = id\big|_{N'} = id'\big|_{N'}$.

and by the previous proposition $id'' = id'$.

Furthermore for every $f \in PR$ and $y \in \mathrm{N}$ $(id'\circ f\circ id')(y) \in N'$ and

$f' = id'\circ f'\circ id'$

so $(\underbrace{id'\circ f\circ id')}(y) = [(\underbrace{id'\circ f\circ id')(}y)]' = [id'\circ f\circ id'\circ \underset{\sim}{y}]' =$

$= id''\circ f'\circ id'\circ \underset{\sim}{y}' = id'\circ f'\circ id'\circ \underset{\sim}{y}'$.

using $(*)$ we got $= id'\circ f'\circ id'\circ \underset{\sim}{y} = f'\circ \underset{\sim}{y} = f'(y)$

i.e. $id'\circ f\circ id' = f'$.

We know that $\mathrm{R}(id') = N' \neq \mathrm{N}$, so $id'\circ id' \neq id$. Moreover $id'(0) = S'^{\square}(0) = 0$ in other words $\mathrm{R}(id') \ni 0$. If id' is a constant function (in other words if there is one element in $\mathrm{R}(id')$ only) then id' must be the function $\underset{\sim}{0}$. Then for every $f \in PR$ $L(f) = \underset{\sim}{0}$ because $f' = id'$ $f' = \underset{\sim}{0}\circ f' = \underset{\sim}{0}$ i.e. $L = \underline{0}$.

Now suppose that $id' \neq \underset{\sim}{0}$, in other words id' is not constant. So we can apply the Lemma 1 choosing $u = v = id'$ because we have seen, that $f' = id'\circ f\circ id'$ for every $f \in PR$ and $id'\circ id' \neq id$. On the Lemma 1 we can say that $L \notin End\langle PR, o\rangle$ so $L \notin End\langle PR, o, \square\rangle$. This contradict to our assumtion and this contradiction proves our theorem. ■

The following corollary shows the importance of this theorem:

COROLLARY: Let $g_1, g_2, \ldots, g_k \in PR$ and $0_1, \ldots, 0_r$ be operations on PR. Suppose that PR can be generated from the functions $g_1, \ldots, g_k$ with the help of operations $0_1, \ldots 0_r$. Further suppose that there is a finite procedure how to calculate the function $f^{\square}$ from the functions $f \in PR$, $g_1, \ldots g_k$ with the help of the above operations. (See the usual proofs of equivalence of the different forms of primitive recursive functions.)

Let $(*)$ denotes the following condition:

$(*)$ $\quad L \in End\langle PR, 0_1, \ldots, 0_r\rangle$ and $L(g_i) = g_i$

for $i = 1, 2, \ldots, k$

If $(*)$ holds then $L\in End\langle PR,o,\square\rangle$ so $L = ID$.
The corollary says that our theorem is true in many usual strucutres of primitive recursive functions.

The proof of Theorem I shows that we used only a few properties of our structure $\langle PR,o,\square\rangle$. This implies the following generalization of this Theorem:

THEOREM I.A. Let $\langle P,o,\square\rangle$ be an <u>arbitrary</u> algebraic structure such that the following axioms hold:

a.) $\langle P,o\rangle$ is a semigroup with unit element id

b.) $\exists! S\in P : S^{\square} = id$

Denote by PS the set of the left-hand-singular elements of $\langle P,o\rangle$ then

c.) $\forall f,\ g\in P : (\forall c\in PS : foc=goc) \Rightarrow f=g$

d.) $\exists c_o \in PS\ \forall f\in P : f^{\square\square} = c_o$

e.) $Vc\in PS\ \exists k_c \in \mathrm{N} : c = \underbrace{SoSo\ldots oSo}_{k_c\ times}c_o$

Then: if $L\in End\langle P,o,\square\rangle$ and $L(id)=id$ then $L=ID$

PROOF: (only sketch) Analogous to the proof of case a.) of Theorem I:

b.) $\Rightarrow L(s)=s$, d.) $\Rightarrow L(c_o)=c_o$

e.) $\Rightarrow Vc\in PS : L(c)=c$ and finally from c.) we get $L(f)=f$ for every $f\in P$ i.e. $L=ID$ ■

This theorem is a generalization of Case a.) only. Theorem I.B below says how to generalize the whole Theorem I in similar way.

THEOREM I.B. Let $\langle P,o,\ \ \rangle$ be an <u>arbitrary</u> algebraic structure and suppose that all the axioms a.) - e.) hold.
Suppose that the following axiom hold too.

f.) if $vou \neq id$, $u\notin PS$ and $L(f)=uofov$ for every $f\in P$ then $L\notin End\langle P,o\rangle$.

Then for every $L \in End<P,o,\square>$ $L=ID$ *or* $L=\underline{0}$

PROOF: (sketch, analogous, to the proof of Theorem I).
There are two cases:
CASE a.) $L(id)=id$, see Theorem I.A.
CASE b.) $L(id)\neq id$.
In this case let $f'=L(f)$ as in the proof of Theorem I.
Let $R(g) := \{g \circ c : c \in PS\}$ for every $g \in P$ (this is the analogue of the range of a function).
Denote by N' the set $\bigcup\{R(g) : g \in P\}$. By the axiom a.) $R(id') = N' \subsetneq PS$ and $id'|_{N'}=id|_{N'}$ and $N'\neq PS$ because $id'\neq id$. By d.) $c'_o=c_o$ and $R(c_o)=\{c_o\}$ because $c_o \in PS$.

<u>Proposition:</u> if $f'|_{N'}=g'|_{N'}$ then $f'=g'$.
Proof: by a.) $f'|_{PS}=g'|_{PS}$ and by c.) $f'=g'$.
Especially for every $c \in PS$ $c'=c$. From this $id''=id'$ follows because $id''|_{N'}=id'|_{N'}$ by a.) and the above proposition. From the above results we get that for every $f \in P$ $f'=id' \circ f \circ id'$, using e.). If $id' \in PS$ then $id'=c_o$, or in other words $L=\underline{0}$.
If $L\neq\underline{0}$ then $id' \notin PS$ and by f.) we get that $L \notin End<P,o>$ i.e. $L \notin <P,o,\square>$. This contradict to our assumption. This contradiction.proves the theorem. ■

At this point some problems arise. For example:
PROBLEM 3. Are the axioms a.) -e.) independent or not?

One can ask similar question about the axioms a.) -f.).
PROBLEM 4. To give more general algebraic form of these theorems above.
Similar problems arise in the next section concerning Theorem II and Theorem III.

GENERATIONS

The main result of this section is Theorem III which is a consequence of Theorem II. Theorem III says that PR^{+} and even PR cannot be generated from one function with the help of our operations o and $\square$. In this section I am dealing with arbitrary functions from N to N, not only functions from PR, except in Theorem III. The proof of Theorem II is made throught some lemmas.

LEMMA 3. Let f be an arbitrary function from N to N. If $f^{\square}$ is not surjective then $R(f^{\square})$is a finite set.

PROOF: It comes from the definition of f that if $f^{\square}(n)=f^{\square}(m)$ for any $m>n$ then $R(f^{\square})=\{f\ (0),\ f^{\square}(1),\dots,f^{\square}(m)\}$.■

REMARK: In the case above $f^{\square}$ is a periodical function and its period is $m-n$. We can ask whether for every periodic function f there is a function g such that $f=g^{\square}$. The answer is the following: Let $a_i=f(i)$, $i\theta$N and the sequence (a_i) is periodic from the place n and its period is $m-n$ (i.e. $\forall j\theta$N $a_{n+j}=a_{m+j}$.) Then there is a function g such that $f=g^{\square}$ if and only if the numbers $a_0,a_1,\dots,a_{m-1}$ all are distinct and $a_0=0$.

Obviously, $f^{\square}$ is bijective if and only if $f^{\square}$is surjective. Moreover it is easy to see that if g is an injective function, $R(g)\not\ni 0$ then $g^{\square}$ is an injective one, too. The following lemmas investigate this problem in more details.

LEMMA 4. If f is not injective then $f^{\square}$ is not surjective.

PROOF: Let $k_1\neq k_2$ and $i=f(k_1)=f(k_2)$.

Suppose that $f^{\square}$ is surjective.

Then there are h_1, $h_2\theta$N such that $k_1=f^{\square}(h_1)$ and $k_2=f^{\square}(h_2)$ and $h_1\neq h_2$.

Then $i=f(k_1)=f(f^{\square}(h_1))=f^{\square}(h_1+1)$ and on similar way we get that $i=f^{\square}(h_2+1)$. We know that $h_1+1\neq h_2+1$ and by Lemma 3 R(*f* is a finite set i.e. *f* is not a surjective function. This contradiction proves the lemma. ■

From this point for an arbitrary function *a* from N to N denote by $\langle a\rangle$ the generation of *a* with the help of the operations o and □ i.e. the set of those functions from N to N which we can built from *a* with the help of the above operations in finite steps.

LEMMA 5. If *a* is an arbitrary injective function then for every element *f* of $\langle a\rangle$

f is injective or *R(f)* is a finite set.

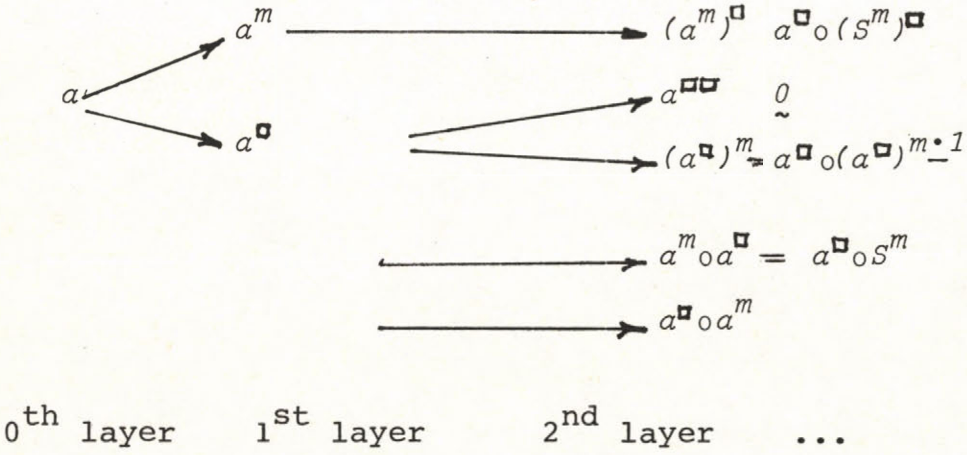
PROOF: Let us investigate how we build the elements of $\langle a\rangle$ in more detail. Then prove the lemma by induction. For every natural number *m* and function *f* from N to N
$f^m \circ f^{\square} = f^{\square}\circ S^m$ and $(f^m)^{\square}=f^{\square}\circ (S^m)$.

Taking these identities into account we get the following scheme, when we construct $\langle a\rangle$ on the basis of the system below:

the 0th layer is $\{a\}$
we get the r+1th layer on the basis of the followings:
first from the elements of the rth layer
using □ or mth power of o
second from the different elements of the rth layer using o
third from the different elements of the rth layer and
layers number less then r using o.

We can see easily with induction on the number of layers that for every element *f* of $\langle a\rangle$ *f* is injective or R*(f)* is a finite set.

(Because if for h and g: h is injective or $R(h)$ is finite and respectively for g then hog and $h^{\square}$ have the same property, too.) ■


a
a^m
$a^{\square}$
$(a^m)^{\square}$ $a^{\square}o(s^m)^{\square}$
$a^{\square\square}$ $\underset{\sim}{0}$
$(a^{\square})^m = a^{\square}o(a^{\square})^{m \dot{-} 1}$
$a^m o a^{\square} = a^{\square} o s^m$
$a^{\square} o a^m$
0th layer
1st layer
2nd layer
...

Scheme

LEMMA 6. For every element f of $\langle a\rangle$ either there is a suitable k such that $f=a^k$ or $R(f)\cdot \subseteq R(a^{\square}\ )$.

PROOF: Similar to the proof of the previous lemma. An induction as above shows how to build the elements of $\langle a\rangle$. We can see easily with induction on the number of layers that for every function f laying in the part of the above figure fenced with dotted line that $R(f) \subseteq R(a^{\square}\ )$. Because for every function g and h $R(hog) \subseteq R(h)$ and $R(g\ \ )\ \_\ R(g)\ \ \{0\}$ furthermore if $R(h) \subseteq R(a)$ then $R(a^m o h)\ \_\ R(a^m o a^{\square}) \subseteq R(a^{\square})$. The reader can prove this lemma in detail himself.

With the help of above lemmas there is no difficulty in proving our main theorems.

THEOREM II. Let a be an arbitrary function from N to N.

Then
either there is no bijection in $\langle a \rangle$
or $\forall f \in \langle a \rangle$ f is injective or $R(f)$ is finite.

PROOF: If a is injective then see Lemma 5.
If a is not injective then a^m is not injective as well. In this case I prove that there is no bijection in $\langle a \rangle$. Proving by indirect way, suppose that there is a bijective element f of $\langle a \rangle$. Since f is injective $f \neq a^m$ for all $m \in$N. But f is surjective and by Lemma 6 $a^{\square}$ must be a surjective function.
By Lemma 4 this is a contradiction, which proves the theorem.

From this theorem it is easy to show the main theorem:

THEOREM III. There is no primitive recursive function such that it can generate all the monoton increasing primitive recursive functions even not all the primitive recursive functions. In other words:

$$\neg \exists a \in PR : \quad \langle a \rangle = PR^{+} \quad or \quad \langle a \rangle = PR$$

PROOF: By Theorem II id and $\underline{\cdot}$ (its definition see in the Introduction) cannot be at the same time in $\langle a \rangle$ for every function a from N to N.
This proves the theorem. ■

One can put the following problem similar to Problem 4:

PROBLEM 5. To give more algebraic form of the above theorems in similar way as it was shown in Theorem I.A and I.B. To solve this problem (other exercise) I suggest to take each element f of P as a function mapping from PS into PS: let $f(c)=f \circ c$ for every element c of PS.

PROBLEM 6. We have seen that for example $\langle S\rangle\_PR^{+}$. So far I have not found any element of $PR^{+}\setminus\langle S\rangle$ yet. So the problem is to show any element of $PR^{+}\setminus\langle S\rangle$.

REMARK: One can investigate other subspaces of PR and prove that they cannot be generated from one element only. For example there is no difficulty in showing that the following subspaces have this property:

$PR_{fin} = \{ f$: $R(f)$ is a finite set $\}$

$PR_{n} = \{ f$: in $R(f)$ there are at most n elements $\}$

$PR_{inj} = \{ f$: f is injective or $R(f)$ is finite $\}$

$PR_{con} = \{ c, c^{\square} : c \in N \}$

$PR_{per} = \{ f$: f is periodic $\}$

$PR_{pern} = \{ f$: f is periodic and its period contains no more than n elements $\}$

$PR_{o} = \{ f : f(0)=0\} = Ker\,\square$

$PR_{bij} = \{ f$: $f(0)$ and f is bijective $\}$

PRsurj= $\{ f$: f is no surjective $\}$

REFERENCES

[1] ROBINSON, R.M. Primitive recursive functions. Bull. Amer. Math. Soc. 1 (1947), 925-942.

[2] PETER,R. Recursive Functions. Akadémia, Budapest, 1967.

[3] ROBINSON,J. General recursive functions. Proc. Amer. Math. Soc. 1 (1950), 703-718.

[4] MONK, D.J. Mathematical Logic. Springer-Verlag, New-York, 1976.

[5] SHOARE, R.I. Recursive enumerable sets and degrees. Bull. Amer. Math. Soc. (1978. nov.) 1149-1162.

[6] HERRINGTON,L. et SHOARE, R.A. Definable degrees and automorphisms of ν. Bull. Amer. Math. Soc. (1981. jan.) 97-99.

A primitiv rekurziv függvények algebrai strukturájáról

Szalkai István

Összefoglalás

E cikkben a primitiv rek. fv.-ek halmazát algebrai strukturaként tekintettem: a kompozició (o) és a 0-tól való iteráció (□) müveletekkel.

Belátom, hogy e strukturában az ID és $\underline{O}$ endomorfizmusokon kivül nincsen más endomorfizmus (ld. I. Tétel).

Ezután részletesen megvizsgálom, hogy N^N mely részhalmazai generálhatók egy függvénnyel a fenti két operáció segitségével. (ld. II. Tétel).
Ebből speciálisan adódik, hogy a prim. rek. függvények halmaza nem generálható egy függvénnyel, (ld. III.Tétel). Néhány idevágó problémát is emlitek, a tételek algebrai általánositásai után.

АЛГЕБРАИЧЕСКАЯ СТРУКТУРА ПРИМИТИВНЫХ РЕКУРСИВНЫХ ФУНКЦИЙ

И. Салкаи

Резюме

Статья занимается множеством примитивных рекурсивных функций как алгебраической структурой. В этой структуре существуют две операции: композиция (о) и итерация с места 0 / □ , см. во Введении/. Доказывается, что над этой структурой существуют только два эндоморфизма: ID и $\underline{0}$. /см. Теорема I./ После этого статья занимается вопросом: какие подмножества N^N /функции из N в N / можно получить из одной функции. /см. Теорема II/.
Из этой теоремы получается важная Теорема III: подмножество примитивных рекурсивных функций нельзя составлять из одной функции. Кроме этих доказываются теоремы в общей алгебраической форме и дано несколько проблем.